Ekwan E. Rhow - State Bar No. 174604
erhow@birdmarella.com
Marc E. Masters - State Bar No. 208375
mmasters@birdmarella.com
Oliver Rocos - State Bar No. 319059
orocos@birdmarella.com
BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100

Jonathan M. Rotter - State Bar No. 234137
jrotter@glancylaw.com
David J. Stone - State Bar No. 208961
dstone@glancylaw.com
GLANCY PRONGAY & MURRAY LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150
Email: info@glancylaw.com

Korey A. Nelson (to be admitted *pro hac vice*)
knelson@burnscharest.com
Amanda K. Klevorn (to be admitted *pro hac vice*)
aklevorn@burnscharest.com
Claire E. Bosarge (to be admitted *pro hac vice*)
cbosarge@burnscharest.com
BURNS CHAREST LLP
365 Canal Street, Suite 1170
New Orleans, LA 70130
Telephone: (504) 799-2845

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

GRACE LAU and CHRISTOPHER KARWOWSKI, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

GEN DIGITAL INC., a corporation, and JUMPSHOT INC., a corporation,

Defendants.

CASE NO.

CLASS ACTION COMPLAINT FOR:

1. **Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, et seq.**
2. **Violation of the California Invasion of Privacy Act, California Penal Code §§ 631 and 632**

(caption continued on next page)

3. **Violation of the Right to Privacy - California Constitution**
4. **Intrusion upon Seclusion**
5. **Statutory Larceny, California Penal Code §§ 484 and 496**
6. **Violation of the California Unfair Competition Law, Bus. & Prof. C. §§ 17200 et seq.**
7. **Unjust Enrichment**

DEMAND FOR JURY TRIAL

Plaintiffs Grace Lau and Christopher Karwowski ("Plaintiffs"), individually and on behalf of a class of similarly situated individuals, by and through their undersigned counsel, allege the following against Gen Digital Inc. ("Gen Digital") and Jumpshot, Inc. ("Jumpshot" and, collectively with Gen Digital, "Defendants"), upon information and belief:

INTRODUCTION

1. This is a case about Defendants' surreptitious electronic surveillance of their customers and invasion of their customers' privacy by intercepting, collecting, and storing customers' Internet search engine keyword searches, search results, and email inbox searches. Defendants' wrongful practice was not disclosed to their customers.

2. What makes this present conduct even more egregious is that after Defendants engaged in similar illegal conduct in the past and were caught doing so, Defendants purported to apologize for their actions, but then secretly revived their past practices in order to continue misappropriating their customers' privacy and data for the sake of profits. Defendants' illegal and persistent misconduct must now be stopped once and for all.

3. Defendants' practices all violate the federal Electronic Communications Privacy Act, the California Invasion of Privacy Act, California's Unfair Competition Law, and other statutory, Constitutional, and common law privacy, data, and consumer protections.

THE SCHEME

4. Defendant Gen Digital is a computer software company, formerly known as Symantec Corp. (1982-2019) and NortonLifeLock Inc. (2019-2022). In 2022, it acquired the entirety of the assets of a company called Avast PLC ("Avast"). It is therefore Avast's successor, and it is responsible for Avast's liabilities.

5. While Avast is no longer an independent company, it continues to operate in much the same way as it did prior to its acquisition. Avast markets itself as a developer of certain software that makes it safer and more secure for users to browse the Internet.

6. But Avast is a data harvester masquerading as a data protector.

7. Avast claims that its products (i) prevent third parties from surreptitiously tracking and collecting the users' browsing activity and personal information and (ii) block malicious

websites that try to steal their data. But Avast does not disclose the fact that, while its software may prevent *third parties* from stealing users' data, its own software steals users' data *for Gen Digital and Avast*.

8. At issue in this action are two Gen Digital and Avast products, the Avast Online Security & Privacy (the "AOSP") and the Avast SafePrice ("SafePrice") browser extensions for the Google Chrome and Microsoft Edge Internet browsers.

9. According to Avast, AOSP protects users' privacy, secures users' browsers against online threats and phishing scams, keeps users' online activities private and anonymous, disguises users' online profile, and prevents tracking on every website the user visits. SafePrice is marketed as providing the best prices, deals, and coupons while shopping online.

10. However, both of these products secretly collect and store the users' data in such a systematic way that they effectively create a "live feed" of millions of users' Internet browsing data.

11. For years, Avast secretly monetized the data it collected from AOSP and SafePrice by selling the data to Avast's own subsidiary, Jumpshot. Jumpshot then sold the data to its customers, including major retailers and marketers.

12. In October 2019, Avast's use of Jumpshot to monetize the data was exposed by third parties, resulting in consumer backlash and governmental scrutiny. In January 2020, Avast acknowledged its practice and shut down Jumpshot.

13. However, Gen Digital and Avast continued to intercept and collect their users' Internet search engine keyword searches, search results, and email inbox searches through AOSP and SafePrice without providing adequate disclosure of its data theft to users.

14. Gen Digital and Avast's users never consented to having Gen Digital and Avast intercept and collect their Internet search engine keyword searches, search results, and email inbox searches. Gen Digital and Avast's practice of monitoring, intercepting, and collecting user information without adequate notice amounts to a massive breach of privacy, and violates statutory, Constitutional, and common law privacy, data, and consumer protections.

15. Gen Digital and Avast's users never consented to the extraction and sale or provision of their detailed Internet browsing data to Gen Digital and Avast, from Avast to Jumpshot, or from

Jumpshot to major retailers and marketers. Avast and Jumpshot's coordinated, undisclosed scheme to profit off Avast's users' personal information without adequate notice amounts to a massive breach of privacy, and violates California statutory larceny law, as well as other statutory, Constitutional, and common law privacy, data, and consumer protections.

THE PARTIES

16. Plaintiff Grace Lau is, and has been, an individual and resident of Alameda, California.

17. Plaintiff Christopher Karwowski is, and has been, an individual and resident of Los Angeles, California.

18. Defendant Gen Digital is a foreign corporation authorized to do business in California. Gen Digital is organized under the laws of the State of Delaware and headquartered in Tempe, Arizona. Although Avast merged with Gen Digital (under its previous name NortonLifeLock) in 2022, Gen Digital continues to sell software under the trade name Avast. When "Avast" is used in this complaint, it refers to Avast and its successor in interest, Gen Digital.

19. Defendant Jumpshot was a Delaware Corporation, registered in California, whose principal office was located at 60 S. Market Street, San Jose, CA, 95113. Avast dissolved Jumpshot in January 2020, but it remains amenable to suit through the California Secretary of State.

JURISDICTION AND VENUE

20. The Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because it involves claims arising under the laws of the United States, including violations of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22. The Court has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

21. The Court also has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) and 1367 because: (i) this is a class action in which the matter in controversy exceeds the sum of $5,000,000, exclusive of interest and costs; (ii) there are 100 or more class members; and (iii) some members of the class are citizens and/or residents of different states than Defendants.

22. The Court has personal jurisdiction over Gen Digital and venue is proper in this District because Gen Digital and Avast's intentional tortious conduct was directed by Gen Digital

and Avast into this District, including toward Plaintiff Lau. Gen Digital does extensive business within the United States, including within this District.

23. Gen Digital and Avast operate a website with substantial interactivity, on which U.S. consumers may download and purchase products, request refunds, and request help on billing and payment inquiries, among other features.

24. Gen Digital and Avast's press releases regarding the products at issue in this case were directed at and issued from Redwood City, California and Emeryville, California.

25. Gen Digital and Avast advertise their products for sale in California.

26. Gen Digital and Avast sponsor the UC Irvine high-school cybersecurity curriculum program.

27. According to Avast's 2019 Annual Report, it "cooperate[s] closely" with California-based research institutions including Stanford, UC Berkeley and UC Irvine.

28. Also, according to its 2019 Annual Report, Avast leased property in Emeryville, California. This particular lease runs through June 2024. Gen Digital and Avast's website highlights its "major office" in Silicon Valley and includes several photos of the Emeryville office workspace.

29. Gen Digital and Avast continuously and deliberately exploit California residents for their own commercial gain.

30. The Court has personal jurisdiction over Jumpshot and venue is proper in this District because it is, or at all relevant times was, headquartered here and because Jumpshot has consented to California law within one or more of its commercial contracts.

31. The Court has personal jurisdiction over Gen Digital and Avast and venue is proper in this District because Jumpshot's tortious conduct was directed by Avast into this District, including toward Plaintiff Lau.

32. In accordance with 28 U.S.C. § 1391, venue is proper in this District because: (i) a substantial part of the conduct giving rise to Plaintiffs' claims occurred in and/or emanated from this District; (ii) Defendants transact business in this District; and (iii) Plaintiff Lau resides in this District.

GENERAL ALLEGATIONS

I. Avast promises consumers privacy but steals their Internet and email activity without disclosing the theft.

33. AOSP is available to consumers for download from the Google Chrome Web Store and the Microsoft Edge Web Store. Gen Digital and Avast's webpage for AOSP proclaims that it helps consumers "[b]rowse with more privacy."[1]

34. Gen Digital and Avast claim that with AOSP, consumers can "[e]asily avoid malicious websites and phishing scams," "[b]lock online trackers and browse anonymously," "[o]ptimize your privacy settings on your favorite platforms," and "[t]ake the hassle out of website cookie permissions."[2] Gen Digital and Avast also claim that AOSP gives consumers "an extra level of real-time threat protection, every time you browse."[3]

35. Gen Digital and Avast tout AOSP's purported Privacy Features, stating that AOSP can "[k]eep your online activities private and anonymous" by keeping consumers' online activity hidden, blocking online "snoops," and by giving step-by-step privacy advice.[4] These privacy features include "Anti-tracking – prevent tracking on every website you visit;" and "Global Privacy Control – stop web companies from collecting and selling your personal data."[5]

36. Prior to November 2021, AOSP was called Avast Online Security ("AOS"). AOS offered protection from fake websites and phishing scams while browsing the Internet. Avast claimed that AOS provided instant ratings for searches, warnings for phishing scams, malicious links and malware, and stopped websites from collecting data and tracking the users' browser history with cookies.

37. These assurances regarding AOSP/AOS were and are, in fact, completely hollow because AOSP continues to intercept, collect, and store users' Internet browsing activity, search

---

[1] https://www.avast.com/avast-online-security#mac (*last accessed November 28, 2022*).

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

engine keyword searches and search results. AOSP also intercepts, collects, and stores users' email inbox searches. The same is true for SafePrice.

38. The SafePrice extension also intercepts, collects, and stores users' Internet browsing activity, search engine keyword searches, and email inbox searches.

39. From this information, Gen Digital and Avast—or any third party to which Gen Digital and Avast may provide the data—can recreate a user's entire web browsing history, in addition to reviewing all of their search queries.

40. As an example of how invasive this data collection can be, Internet and email searches by individuals can disclose such personal information as sexual preferences, political leanings, medical conditions or symptoms or illnesses (including abortion services), financial data, and much more. By collecting such searches, Gen Digital and Avast can collect a trove of information about the user, all while representing that they are protecting the user from such information being collected.

II. Avast has an established history of collecting and selling its users' data to third parties.

41. Previously, Avast licensed data it intercepted and collected to its subsidiary,[6] Jumpshot, which in turn sold the data to third party customers including Home Depot and Market Beyond. Those customers could and did use that data, either to better target their advertising or to repackage it before reselling it to others.[7] The insight the data gave Jumpshot's customers into users' web browsing habits gave purchasers of that data such a commercial advantage that Jumpshot even sold information to investors looking for an informational advantage in the public securities markets.[8]

---

[6] Avast acquired 100% of Jumpshot on September 24, 2013. It sold 35% of Jumpshot to Ascential on July 22, 2019. The sale to Ascential was reversed less than a year later when Avast repurchased the 35% interest. The repurchase transaction was completed on January 30, 2020.

[7] *See* Complaint filed in *Deals Way Ltd. v. Jumpshot Inc*., Case No. 3:20-CV-02988, (N.D. Cal. Filed April 30, 2020) ("Deals Way Compl.") ¶ 4.

[8] Thomas Brewster, *Are You One Of Avast's 400 Million Users? This Is Why It Collects And Sells Your Web Habits*, FORBES (Dec. 9, 2019) https://www.forbes.com/sites/thomasbrewster/2019/12/09/are-you-one-of-avasts-400-million-users-this-is-why-it-collects-and-sells-your-web-habits/#180aee4d2bdc.

42. Avast acquired Jumpshot on September 24, 2013. It heralded the acquisition as one that would help keep consumer's data safe and their computers running at peak performance.[9]

43. At the time of the acquisition, Jumpshot's focus was on an application that purportedly made a consumer's computer run more efficiently by decluttering and removing so-called "junk files" from a user's computer.[10]

44. But over time, and in close coordination with its parent entity, Jumpshot expanded into the business of monetizing the consumer data that Avast collected. To achieve that goal, Avast and Jumpshot entered into a licensing agreement pursuant to which Avast licensed to Jumpshot the consumer data it had collected, and which it claimed to own.[11] In return, Jumpshot paid a fee to Avast for the data.

45. Avast knew that Jumpshot was selling the user data to third parties.

46. Avast failed to prohibit Jumpshot from selling that data, or to impose (or ensure Jumpshot adhered to) any meaningful limits on Jumpshot's use of the data it licensed to Jumpshot. And, at all relevant times, Avast maintained control over Jumpshot.

47. Avast did not disclose to its users that their data was being sold by Jumpshot. Unbeknownst to Avast users, Jumpshot promised prospective corporate customers that they could use the data acquired from Avast to "jump the garden wall."[12] The "garden wall" is a term used to describe the universe of websites that Avast users access,[13] and at the time, Jumpshot claimed that it was "the only company that unlocks walled garden data."[14] In other words, while in the ordinary

---

[9] *Id.*

[10] *Id.*

[11] Deals Way Compl. ¶32 (citing February 24, 2020, letter from Jumpshot CEO, Deren Banker).

[12] https://web.archive.org/web/20190205185953/https://www.jumpshot.com/proof_category/data-report/

[13] *See generally* Andrew Froehlich, *What is a walled garden on the internet?*, TECHTARGET (last updated Nov. 2021) https://searchsecurity.techtarget.com/definition/walled-garden.

[14] *Jumpshot Strikes Strategic Partnership Deal with Ascential to Provide Marketers with Deeper Visibility into the Entire Online Customer Journey*, PRNEWSWIRE (July 22, 2019) http://www.prnewswire.com/news-releases/jumpshot-strikes-strategic-partnership-deal-with-ascential-to-provide-marketers-with-deeper-visibility-into-the-entire-online-customer-journey-300888439.html?tc=eml_cleartime.

course a company would not have access to user activity on a competitor's website, Jumpshot was in the business of providing that data.

48. Jumpshot represented that, once in the walled garden, its customers would have access to "incredibly detailed clickstream data from 100 million global online shoppers and 20 million global app users."[15] Jumpshot promised advertisers that they could "track what users searched for, how they interacted with a particular brand or product, and what they bought."[16] Jumpshot encouraged business entities to "[l]ook into any category, country, or domain."[17]

49. This highly personal user information was so useful to Jumpshot's clients—who could use it to direct their advertising far more efficiently[18]—that Avast and Jumpshot could sell it for huge sums.

50. In total, Avast's licensing of data to Jumpshot yielded more than $20 million in annual revenue for Avast.[19]

51. Avast's data collection and monetization strategy through Jumpshot began to unravel in late 2019. On October 28, 2019, Wladimir Palant, a cybersecurity journalist, published a report detailing the personal information Avast collected from its users. This included: (1) every website visited, alongside a user ID;[20] (2) how the user got to the page, such as by clicking on a link, or typing the address manually;[21] (3) the user's country code;[22] (4) the user's unique ID;[23] (5) what

---

[15] Brewster, *supra* note 9.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] Michael Kan, *The Cost of Avast's Free Antivirus: Companies Can Spy on Your Clicks*, PCMAG (Jan. 27, 2020), https://www.pcmag.com/news/the-cost-of-avasts-free-antivirus-companies-can-spy-on-your-clicks.

[21] Wladimir Palant, *Avast Online Security and Avast Secure Browser are spying on you*, ALMOST SECURE (Oct. 28, 2019) https://palant.info/2019/10/28/avast-online-security-and-avast-secure-browser-are-spying-on-you/.

[22] *Id.*

[23] *Id.*

type of browser was used;[24] and, (6) in the case of the Avast antivirus product, the user's operating system and exact version number.[25]

52. Palant concluded that the mosaic of collected information could be used by Avast to answer the following questions:

a. "how many tabs do you have open"?[26]

b. "what websites do you visit and when, how much time do you spend reading/watching the contents"?[27] and

c. "what do you click there and when do you switch to another tab"?[28]

53. Palant further concluded that users who log into their social media accounts can be deanonymized with high precision.[29] Put differently, whoever obtains the data that Avast collects can cross reference a consumer's browsing history with a user's social media account and thus easily determine who the user is and what they are viewing online—down to each click of the mouse.

54. A little over a month after Palant's revelation, Mozilla—the maker of the popular web browser Firefox—learned of Avast's practices and, less then twenty-four hours later, removed four Avast security extensions.[30]

55. On January 27, 2020, *Vice* published an investigative piece titled *Leaked Documents Expose the Secretive Market for Your Web Browsing Data*, reporting that, "[a]n Avast antivirus subsidiary sells 'Every search. Every click. Every buy. On every site.'"[31] The article claimed that

---

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] Catalin Cimpanu, *Mozilla removes Avast and AVG extensions from add-on portal over snooping claims*, (Dec. 3, 2019) https://www.zdnet.com/article/mozilla-removes-avast-and-avg-extensions-from-add-on-portal-over-snooping-claims/.

[31] Joseph Cox, *Leaked Documents Expose the Secretive Market for Your Web Browsing Data*, VICE (Jan. 27, 2020) https://www.vice.com/en_us/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation.

its findings are supported by leaked Avast documents, including contracts, internal product handbooks, and leaked consumer data.[32]

56. Some of that leaked consumer data revealed that Avast was selling information about consumers' personal web browsing history. That browsing history included information such as which pornographic sites a user visited, how long that user stayed there, and what type of pornography that user searched for. And, because the purchaser of such information was able to deanonymize the user, it was even possible for the data buyer to determine whether, for instance, an Avast user had a different sexual preference than what he or she has disclosed to the public (i.e., whether someone was gay or straight, whether out or closeted).[33]

57. The leaked data also showed that Avast was collecting search queries of specific locations, including GPS coordinates on Google maps.[34] In essence, Avast was collecting information about the precise location of where a consumer would be visiting.

58. The *Vice* piece further explained that after Avast collected a consumer's data and licensed it to Jumpshot, Jumpshot sliced, repackaged and sold the data, at times receiving millions of dollars for revealing consumers' "all clicks feed."[35] The Avast source reportedly described the data as being "very granular, and [] great data for these companies, because it's down to the device level with a timestamp."[36] It was also revealed that over 100 million devices had been impacted by Avast's data collection scheme.[37] As of August 2019, Jumpshot advertised having access to "100 million panelists in 188 countries."[38]

59. In short, while Avast was promising its users that its data would be safe and secure from data harvesters, it was harvesting such highly granular and specific information that Jumpshot

---

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] Available on web archive service, the Wayback Machine, available at:https://web.archive.org/web/20190716080831/https://www.jumpshot.com/

advertised to its customers, without exaggeration, as offering the "most precise way to unlock human behavior online."[39]

60. Once Avast's business partners learned of Avast's data collection and disclosure scheme, they quickly severed ties with Avast. For example, shortly after Palant's analysis was published, but before the *Vice* revelations, three major technology companies parted ways with Avast. As noted above, Mozilla discontinued its use of the Avast browser extension on December 3, 2019.[40] Technology firm Opera did the same within 16 hours of learning of Palant's analysis.[41] Roughly two weeks later, on December 18, 2019, Google removed three different Avast browser extensions from the Chrome Web Store.[42]

61. The reason other technology companies quickly pulled the plug on Avast is clear: selling such private data without users' consent is a highly intrusive invasion of privacy. The media articles highlighted the severity of Avast's intrusion upon its 400 million customers and the other technology companies did not want to be tarred with Avast's betrayal of its users' trust, much less its violations of the law.

62. Though Avast has claimed that the data it collects "is fully de-identified and aggregated and cannot be used to personally identify or target" a particular user, multiple studies have shown that it is impossible to truly "anonymize" data.

63. A 2017 study found that web browsing histories can be linked to social media profiles using only publicly available data.[43] After developing a model for web browsing behavior, researchers were able to correctly identify 70% of users based on their web browsing histories.

64. By 2019, another group of researchers had developed a model that correctly

---

[39] Available on web archive service, the Wayback Machine, available at: https://web.archive.org/web/20190205175940/https://www.jumpshot.com/campaign-optimization/

[40] Cimpanu, *supra* note 30.

[41] Wladimir Palant, *Mozilla and Opera remove Avast extensions from their add-on stores, what will Google do?*, ALMOST SECURE (Dec. 3, 2019), https://palant.info/2019/12/03/mozilla-removes-avast-extensions-from-their-add-on-store-what-will-google-do/.

[42] Cimpanu, *supra* note 30.

[43] Jessica Su ET AL., *De-anonymizing Web Browsing Data with Social Networks*, (2017) https://www.cs.princeton.edu/~arvindn/publications/browsing-history-deanonymization.pdf.

identified 99.98% of Americans in any dataset using 15 demographic attributes.[44] The researchers concluded that the study's results "seriously challenge the technical and legal adequacy of the de-identification release-and-forget model."[45]

65. The combination of widespread and well-founded media criticism of Avast, coupled with the product distancing by market participants, pressured Avast into damage control mode. On January 30, 2020, Avast admitted (some but not all of) its improper practices and apologized.[46]

66. Avast also announced its plan to cease the provision of its users' data to Jumpshot and wind down Jumpshot's operations.[47]

67. In response to Avast's announcement that it would wind down Jumpshot, Senator Ron Wyden noted that while "it is encouraging that Avast has ended some of its most troubling practices after engaging constructively with my office," he was still "concerned that Avast has not yet committed to deleting user data that was collected and shared without the opt-in consent of its users, or to end the sale of sensitive internet browsing data."[48]

III. Avast continues to steal its users' personal web browsing information.

68. Although Avast shuttered Jumpshot after its misuse of user data was exposed in late 2019 and early 2020, Gen Digital and Avast continue to intercept and collect users' Internet and email search and browsing activities, without providing adequate notice.

69. Here is how it works: The Avast software is designed to intercept all communications from a main channel (the web browser) between the user and the websites the user visits, and copy those communications to an Avast server.

70. For example, when a user runs a search on Google's search engine, a main channel

---

[44] Luc Rocher ET AL., *Estimating the success of re-identifications in incomplete datasets using generative models*, (July 23, 2019), https://www.nature.com/articles/s41467-019-10933-3.

[45] *Id.*

[46] Avast, *A message from Avast's CEO*, (Jan. 30, 2020) https://blog.avast.com/a-message-from-ceo.

[47] Press Release, Avast, *Avast to Commence Wind Down of Subsidiary Jumpshot*, (Jan. 30, 2020) https://press.avast.com/avast-to-commence-wind-down-of-subsidiary-jumpshot.

[48] Cox, *supra* note 31.

is established between the user and Google to transmit communications such as search queries. The main channel communications are intercepted by AOSP (or AOS) and a copy of the communication is immediately transmitted to Gen Digital and Avast servers, and Gen Digital and Avast store the intercepted data.

71. Similarly, when a user runs a search within their Gmail or Yahoo! email inbox, a main channel is created between the email user and Google or Yahoo and any search conducted by the email user is immediately intercepted by AOSP (or AOS). A copy of the search is immediately transmitted to Gen Digital and Avast servers, and Gen Digital and Avast store the intercepted data.

72. The SafePrice extension also captures Internet searches and searches within users' email inboxes.

73. In light of the very names of the Avast Online Security & Privacy and SafePrice products, as well as Gen Digital and Avast's repeated representations highlighted above regarding how these products purportedly protect users' personal information, consumers are led to believe that their private Internet and email searches and browsing activity are safe.

NAMED PLAINTIFF ALLEGATIONS

74. Plaintiff Grace Lau used both AOSP and SafePrice, both on the Chrome web browser, for years, through mid-2021. Ms. Lau believed that using Avast Online Security & Privacy would help protect her privacy, and she was unaware that Avast was intercepting and collecting her Internet search engine keyword searches, search results, and email inbox searches. Ms. Lau would not have used the Avast products had she known that they were invading her privacy.

75. Plaintiff Lau has incurred harm as a result of Defendants' invasion of her privacy rights through the unauthorized interception, collection, and use of her Internet search engine keyword searches, search results, and email inbox searches.

76. Plaintiff Christopher Karwowski used both AOSP and SafePrice, both on the Chrome web browser, from 2019-2020. Mr. Karwowski believed that using Avast Online Security & Privacy would help protect his privacy, and was unaware that Avast was taking his Internet search engine keyword searches, search results, and email inbox searches. Mr. Karwowski would not have used the Avast products had he known that they were invading his privacy

77. Plaintiff Karwowski has incurred harm as a result of Defendants' invasion of his privacy rights through the unauthorized interception, collection, and use of his Internet search engine keyword searches, search results, and email inbox searches.

CHOICE OF LAW

78. California's substantive laws may be constitutionally applied to the Plaintiffs' and the Nationwide Class members' claims under the Due Process Clause, 14th Amend., § 1, and the Full Faith and Credit Clause, art. IV., § 1, of the U.S. Constitution.

79. California has a significant contact, or significant aggregation of contacts, to the claims asserted by each Plaintiff, thereby creating state interests that ensure that the choice of California state law to the common-law claims is not arbitrary or unfair. Gen Digital and Avast conducted substantial business in California, and Jumpshot was headquartered in California. California has a strong interest in regulating Gen Digital, Avast, and Jumpshot's conduct under its laws.

80. The application of California law to the proposed Nationwide Class members (defined below) is also appropriate under California's choice of law rules, namely, the governmental interest test California uses for choice-of-law questions. California's interest would be the most impaired if its laws were not applied.

TOLLING, CONCEALMENT, AND ESTOPPEL

81. The statutes of limitations applicable to Plaintiffs' claims are tolled as a result of Gen Digital and Avast's knowing and active concealment of their conduct alleged herein.

82. Among other things, as set forth above, Gen Digital and Avast made misleading statements, including in the very titles of the extensions ("Online Security and Privacy" and "SafePrice"), and after a January 2020 investigation revealed Avast had been harvesting user data for sale to third parties ("the Jumpshot investigation"), Gen Digital and Avast intentionally concealed the true nature of their ongoing user data collection practices.

83. Plaintiffs and Class and Subclass members were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their own part.

84. Gen Digital, Avast, and Jumpshot were under a duty to disclose the true character,

quality, and nature of their activities to Plaintiffs and the Class and Subclass members. Gen Digital, Avast, and Jumpshot therefore are estopped from relying on any statute of limitations.

85. All applicable statutes of limitation also have been tolled by operation of the discovery rule. Specifically, Plaintiffs and other Class and Subclass members could not have learned through the exercise of reasonable diligence of Gen Digital, Avast, and Jumpshot's conduct as alleged herein.

86. Gen Digital, Avast, and Jumpshot's fraudulent concealment and omissions are common to Plaintiffs and the Class and Subclass members.

CLASS ACTION ALLEGATIONS

87. Plaintiffs incorporate by reference all of the foregoing allegations.

88. Plaintiffs bring this lawsuit pursuant to Rules 23(b)(2) and (3) of the Federal Rules of Civil Procedure.

89. Plaintiffs seek to represent the following Classes:

> **Nationwide Class:** All natural persons in the United States who used a web browser with the Avast Online Security & Privacy and/or Avast SafePrice browser extension installed.
>
> **California Subclass:** All natural persons residing in California who used a web browser with the Avast Online Security & Privacy and/or Avast SafePrice browser extension installed.

90. Excluded from the Class and Subclass are Defendants, their current employees, co-conspirators, officers, directors, legal representatives, heirs, successors and wholly or partly owned subsidiaries or affiliated companies, and the Judge and court staff to whom this case is assigned.

91. The Class and Subclass and their counsel satisfy the prerequisites of Federal Rule of Civil Procedure 23(a) and 23(g) and the requirements of rule 23(b)(3).

i. Numerosity and Ascertainability:

92. Plaintiffs do not know the exact size of the Class or Subclass or the identities of their members. Such information is known to Defendants. At minimum, each Class and Subclass has many thousands of members. Reports indicate that AOSP and SafePrice have each been installed more than 10 million times from the Chrome Web Store. Reports indicate that AOSP has been installed more than 1 million times from the Edge Add-ons store and SafePrice has been installed

more than 600,000 times from the Edge Add-ons store. Thus, the number of members in the Class and Subclass is so numerous that joinder of all Class or Subclass members is impracticable. Membership of the Class and Subclass is defined using objective criteria and individual members will be identifiable from Defendants' records.

ii. Commonality and Predominance:

93. Common questions of law and fact exist as to all members of the Class and Subclass and predominate over questions affecting only individual members of the Class and Subclass, including the following:

a. Whether Gen Digital and Avast intercepted, received, and/or collected electronic communications of user information, browsing history, search history, and/or web activity from Plaintiffs and Class and Subclass members during the class period;

b. Whether Gen Digital and Avast falsely represented to the public, including Plaintiffs and Class and Subclass members, that it would stop its admitted practice of intercepting, receiving, and/or collecting electronic communications of user information, browsing history, search history, and web activity after the 2020 Jumpshot investigation;

c. Whether Gen Digital and Avast's practice of intercepting, receiving, and/or collecting electronic communications of user information, browsing history, search history, and/or web activity violates state and federal privacy laws;

d. Whether Gen Digital and Avast's practice of intercepting, receiving, and/or collecting electronic communications of user information, browsing history, search history, and/or web activity violates state and federal anti-wiretapping laws;

e. Whether Gen Digital and Avast's practice of intercepting, receiving, and/or collecting electronic communications of user information, browsing history, search history, and/or web activity violates any other state and federal tort laws;

f. Whether Gen Digital and Avast omitted or concealed material facts from Plaintiffs and Class and Subclass members about its practice of intercepting, receiving, and/or collecting electronic communications of user information, browsing history, search

history, and/or web activity;

g. Whether Gen Digital, Avast, and Jumpshot owe a duty to Plaintiffs and Class and Subclass members to disclose material facts about their practice of intercepting, receiving, collecting, and/or using electronic communications of user information, browsing history, search history, and/or web activity;

h. Whether Gen Digital, Avast, and Jumpshot's conduct described herein violates Plaintiffs' and Class and Subclass members' interest in precluding the dissemination or misuse of sensitive and confidential information ("informational privacy");

i. Whether Gen Digital, Avast, and Jumpshot's conduct described herein violates Plaintiffs' and Class and Subclass members' interest in making intimate personal decisions or conducting activities without observation, intrusion, or interference ("autonomy privacy");

j. Whether Gen Digital, Avast, and Jumpshot improperly obtained and/or disclosed Plaintiffs' and Class and Subclass members' data without authorization or in excess of any authorization;

k. Whether profits obtained by Gen Digital, Avast, and Jumpshot through the sale of information or sale of access to information that they obtained from Plaintiffs and Class and Subclass members were unjustly obtained and should be disgorged;

l. Whether any profits or other value obtained by Gen Digital, Avast, and Jumpshot through analysis, enrichment, and other use of information from Plaintiffs and Class and Subclass members were unjustly obtained by Gen Digital, Avast, and Jumpshot, and should be disgorged;

m. Whether Plaintiffs and Class and Subclass members sustained damages as a result of Gen Digital, Avast, and Jumpshot's conduct, and, if so, what is the appropriate measure of damages or restitution; and

n. Whether Plaintiffs and Class and Subclass members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein.

94. Gen Digital, Avast, and Jumpshot engaged in a common course of conduct giving rise to the legal rights sought to be enforced by this action. Furthermore, similar or identical questions of statutory and common law, as well as similar or identical injuries, are involved. Individual questions, if any, pale in comparison to the numerous common questions that predominate in this action.

iii. Typicality:

95. Plaintiffs' claims are typical of the claims of other Class and Subclass members because, among other things, all members of the Class and Subclass were uniformly affected by Defendants' wrongful conduct in violation of federal and state laws as complained of herein.

iv. Adequacy of Representation:

96. Plaintiffs will fairly and adequately protect the interests of the Class and Subclass. Plaintiffs have retained counsel experienced in complex class actions and data privacy litigation, and Plaintiffs intend to vigorously prosecute this case on behalf of the Class and Subclass. Further, Plaintiffs have no interests that are antagonistic to the Class and Subclass.

v. Superiority:

97. A class action is superior to individual litigation and all other available methods for the fair and efficient adjudication of this controversy. The damages suffered by individual members of the Class and Subclass are relatively small compared to the burden and expense required to individually litigate claims against Defendants. It would thus be impossible for members of the Class and Subclass, on an individual basis, to obtain effective redress for the wrongs committed against them.

98. Moreover, individualized litigation presents the potential for inconsistent or contradictory judgments, and increases the delay and expense presented by the complex legal and factual issues of the case to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

(Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *Et Seq.* Against Gen Digital)

99. Plaintiffs, individually and on behalf of the Class and Subclass, incorporate the foregoing allegations as if fully set forth herein.

100. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, proscribes the intentional interception, disclosure, or use of the contents of any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

101. The statute provides a private right of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

102. The Federal Wiretap Act protects both the sending and receipt of electronic communications.

103. Plaintiffs and Class and Subclass members, as individuals, are persons within the meaning of 18 U.S.C. § 2510(6).

104. When Plaintiffs or Class and Subclass Members install AOSP or SafePrice extensions, Gen Digital and Avast intercept communications between Plaintiffs and Class and Subclass members, on the one hand, and the search engines they use and websites that they visit, on the other. Gen Digital and Avast's interception of those communications is intentional. Gen Digital and Avast are sophisticated software companies that know their products are intercepting communications in these circumstances and have taken no remedial action.

105. Gen Digital and Avast's interception of the communications is while the Plaintiffs' and Class and Subclass members' communications are in transit or in the process of being sent or received to and from the search engines and websites to which they navigate.

106. The Federal Wiretap Act defines "contents" as including "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). The communications intercepted by Gen Digital and Avast include "contents" of electronic

communications exchanged between Plaintiffs and Class and Subclass members, on the one hand, and the search engines and other websites to which they navigated, on the other, in the form of detailed URL requests, webpage browsing histories and search queries, URLs containing the specific search term(s) communicated to the search engine, and email inbox search queries. Plaintiffs and Class and Subclass members sent communications to those search engines and websites, and Plaintiffs and Class and Subclass members received communications in return from those search engines and websites.

107. The transmission of data between Plaintiffs and Class and Subclass members, on the one hand, and the search engines and websites with which they chose to exchange communications, on the other, constitutes the "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce." The transmitted data is therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

108. Gen Digital and Avast intercept the electronic communications while they are in transit by using software that automatically duplicates the communication between the user and the search engine or website and sends the duplicated information to Gen Digital and Avast's servers.

109. The communications between the Plaintiffs and Class and Subclass members, on the one hand, and search engines and websites, on the other, were simultaneous to, but separate from, the channel through which Gen Digital and Avast acquired the contents of those communications.

110. The following constitute "devices" as defined under § 2510(5) of the Act:

a. The web browsers of Plaintiffs and Class and Subclass members;

b. The personal computing devices of Plaintiffs and Class and Subclass members;

c. The computer codes and programs used by Gen Digital and Avast to effectuate the interception of the communications that are exchanged between search engines and websites, on the one hand, and Plaintiffs and Class and Subclass members, on the other, while browsing the Internet on a web browser with AOSP and/or SafePrice extensions installed;

d. Gen Digital and Avast's servers;

e. The servers of websites and search engines from which Gen Digital and Avast intercepted the communications sent or received by Plaintiffs and Class and Subclass members; and

f. The plan Gen Digital and Avast carried out to effectuate the interception of the communications that are exchanged between search engines or websites, on the one hand, and Plaintiffs and Class and Subclass members, on the other, while browsing the Internet on a web browser with AOSP and/or SafePrice extensions installed.

111. For purposes of this Complaint, Gen Digital and Avast are not "electronic communication service[s]," as defined in 18 U.S.C. § 2510(12), nor are Gen Digital and Avast Internet Service Providers.

112. Gen Digital and Avast's unlawful interception of electronic communications is not excused under 18 U.S.C. § 2511(2)(c) because Gen Digital and Avast are not parties to the communication and have not received prior consent from the website, search engines, Plaintiffs, or Class or Subclass members to engage in such interception.

113. Neither the Plaintiffs nor Class or Subclass members were aware that Gen Digital and Avast were intentionally intercepting communications between Plaintiffs and Class or Subclass members, on the one hand, and the search engines and websites that they use on web browsers with the AOSP and/or SafePrice extensions installed, on the other. Likewise, the websites that Plaintiffs and Class and Subclass members visited did not know of or consent to Gen Digital and Avast's interception of the details about visitors' access to and activities on their websites.

114. For the violations set forth above and pursuant to 18 U.S.C. § 2520, Plaintiffs and members of the Class and Subclass seek (1) appropriate preliminary and other equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and Class and Subclass members and any profits made by Defendants as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; (3) punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Gen Digital and Avast in the future; and (4) reasonable attorney's fees and other litigation costs reasonably incurred.

SECOND CAUSE OF ACTION

(Violation of the California Invasion of Privacy Act, California Penal Code §§ 630, *et seq.* Against Gen Digital)

115. Plaintiffs, individually and on behalf of the Class and Subclass, incorporate the foregoing allegations as if fully set forth herein.

116. The California Invasion of Privacy Act ("CIPA"), codified at Cal. Penal Code §§ 630 to 638, begins by providing its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

117. California Penal Code § 631(a) imposes liability upon:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section . . . .

Section 631(a) applies to communications conducted over the Internet.

118. California Penal Code § 632(a) imposes liability upon:

> A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio . . . .

119. Under both section 631(a) and section 632(a), the alleged violator must show it had the consent of all parties to a communication to avoid liability.

120. At all relevant times, Gen Digital and Avast's interceptions of the Plaintiffs' and Class and Subclass members' Internet communications in transit originating in or sent to California were and are without the authorization or consent of the Plaintiffs, the Class and Subclass Members, and the websites and search engines with which they communicated. Gen Digital and Avast were not participants to the communications and the interceptions by Gen Digital and Avast in the aforementioned circumstances were and are unlawful and tortious.

121. Plaintiffs and Subclass members were in California during one or more of their internet usage sessions in which Defendants stole their data. Upon information and belief, each Class member, even those located outside of California, during one or more of their interactions on the Internet during the applicable statute of limitations period, communicated with one or more entities based in California, and/or with one or more entities whose servers were located in California. Communications from the California web-based entities to Class members were sent from California. Communications to the California web-based entities from Class members were sent to California.

122. Plaintiffs and Class and Subclass members did not consent to any of Gen Digital and Avast's actions in intercepting, reading, and/or learning the contents of their communications with such California-based entities.

123. Gen Digital and Avast's non-consensual interception of the Plaintiffs' and Class and Subclass members' Internet communications while they were using web browsers with AOSP and/or SafePrice extension installed was designed to attempt to learn at least some meaning of the content in the communication between Plaintiffs and Class and Subclass members, on the one hand, and the websites and search engines to which they navigated, on the other.

124. The communications intercepted by Gen Digital and Avast include "contents" of electronic communications exchanged between Plaintiffs and Class and Subclass members, on the one hand, and the search engines and other websites to which they navigated, on the other, in the form of detailed URL requests, webpage browsing histories and search queries, URLs containing

the specific search term(s) communicated to the search engine, and email inbox search queries. Plaintiffs and Class and Subclass members sent communications to those search engines and websites, and Plaintiffs and Class and Subclass members received communications in return from those search engines and websites.

125. The following items constitute "machine[s], instrument[s], or contrivance[s]" under § 631(a), and even if they did not, Gen Digital and Avast's deliberate and admittedly purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

a. The Plaintiffs' and Class and Subclass members' browsers;

b. The Plaintiffs' and Class and Subclass members' personal computing devices;

c. The computer codes and programs used by Gen Digital and Avast to effectuate the interception of communications exchanged between websites and search engines, on the one hand, and Plaintiffs and Class and Subclass members, on the other, while browsing the Internet on a web browser with AOSP and/or SafePrice extensions installed;

d. Gen Digital and Avast's servers;

e. The servers of websites and search engines from which Gen Digital and Avast intercepted the Plaintiffs' and Class and Subclass members' communications; and

f. The plan Gen Digital and Avast carried out to effectuate the interception of the communications that are exchanged between websites and search engines, on the one hand, and Plaintiffs and Class and Subclass members, on the other, while browsing the Internet on a web browser with AOSP and/or SafePrice extensions installed.

126. The data collected by Gen Digital and Avast constituted "confidential communications," as that term is used in § 632(a), because Plaintiffs and Class and Subclass members have an objectively reasonable expectation of privacy that their private browsing communications are not being intercepted or disseminated.

127. Plaintiffs and Class and Subclass members have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their

personally-identifiable information.

128. Pursuant to California Penal Code § 637.2, Plaintiffs and Class and Subclass members have been injured by the violations of California Penal Code §§ 631 and 632, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive or other equitable relief.

THIRD CAUSE OF ACTION

(Invasion of Privacy Under Article I, Section 1 of the California Constitution Against All Defendants)

129. Plaintiffs, individually and on behalf of the Class and Subclass, incorporate the foregoing allegations as if fully set forth herein.

130. In 1972, California added a right of privacy to the list of enumerated inalienable rights in Article I, § 1 of its Constitution.

131. To plead invasion of privacy under the California Constitution, Plaintiffs must allege "that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is 'so serious . . . as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020), quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009).

132. Plaintiffs and Class and Subclass members have a legally protected privacy interest in:

a. precluding the collection, copying, dissemination and/or misuse of their sensitive, confidential personally-identifiable information; and

b. making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various Internet sites without having that information intercepted and transmitted to Defendants without their knowledge or consent.

133. Based on the names of the products ("Online Security and Privacy" and "SafePrice"), Plaintiffs and Class and Subclass members had a reasonable expectation of privacy in the personally identifiable information Defendants collect without adequately notifying users.

134. Defendants' actions constitute a serious invasion of privacy in that they are:

a. Invading a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices, including web search and browsing histories;

b. Violating several federal criminal laws, including the Electronic Communications Privacy Act;

c. Invading the privacy interests and rights of millions of Americans (including Plaintiffs and Class and Subclass members) without their consent;

d. Engaging in the unauthorized taking of valuable information from millions of Americans through deceit; and

e. Committing criminal acts against millions of Americans, which constitutes an egregious breach of social norms that is highly offensive.

135. The surreptitious and unauthorized interception of the Internet communications of millions of Americans who have taken active measures to ensure their privacy by installing Gen Digital and Avast's extensions, constitutes an egregious breach of social norms that is highly offensive.

136. Defendants' intentional intrusion into Plaintiffs' and Class and Subclass members' Internet communications and their computing devices and web browsers is highly offensive to a reasonable person in that Defendants violated federal and state criminal and civil laws designed to protect individual privacy and guard against theft.

137. The unauthorized taking of personally-identifiable information from millions of Americans through deceit is highly offensive behavior.

138. The secret monitoring of private Internet browsing is highly offensive behavior.

139. Wiretapping and surreptitious recording of communications is highly offensive behavior.

140. Defendants lacked a legitimate business interest in intercepting and receiving private Internet communications between Plaintiffs and Class and Subclass members, on the one hand, and the search engines and websites to which they navigated, on the other, without first obtaining the

consent of Plaintiffs, Class and Subclass members, or the websites and search engines.

141. Plaintiffs and Class and Subclass members have sustained, and will continue to sustain, damages as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation and injunctive relief, as well as such other relief as the Court may deem just and proper.

FOURTH CAUSE OF ACTION

(Intrusion Upon Seclusion
Against All Defendants)

142. Plaintiffs, individually and on behalf of the Class and Subclass, incorporate the foregoing allegations as if fully set forth herein.

143. A claim for intrusion upon seclusion requires (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

144. By intercepting the Internet communications of Plaintiffs and Class and Subclass members, Defendants intentionally intruded upon their solitude or seclusion.

145. Gen Digital and Avast intentionally intruded upon Plaintiffs' and Class and Subclass members' solitude, seclusion, and private affairs by intentionally designing their extensions and programming code to surreptitiously intercept and retain the private and personally-identifiable information of Plaintiffs and Class and Subclass members. Gen Digital and Avast effectively place themselves in the middle of conversations to which they are not an authorized party. Jumpshot intentionally intruded upon Plaintiffs' and Class and Subclass members' solitude, seclusion, and private affairs by intentionally receiving and using this information, knowing how it had been obtained.

146. Defendants intercept these Internet communications without authority or consent from Plaintiffs, Class and Subclass members, or the websites and search engines with which they communicate.

147. Defendants' intentional intrusion into Plaintiffs and Class and Subclass members' Internet communications, computing devices, and web browsers is highly offensive to a reasonable person in that such intrusions violate federal and state criminal and civil laws designed to protect individual privacy and guard against theft.

148. The unauthorized taking of personally-identifiable information from millions of Americans through deceit is highly offensive behavior.

149. The secret monitoring of private Internet browsing is highly offensive behavior.

150. Wiretapping and surreptitious recording of communications is highly offensive behavior.

151. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions.

152. Plaintiffs and Class and Subclass members reasonably expected that their personal data would not be intercepted, collected, stored, or used by Defendants.

153. Plaintiffs and Class and Subclass members have been damaged by these intrusions, which have allowed Defendants to obtain profits that rightfully belong to Plaintiffs and Class and Subclass members. Plaintiffs and Class and Subclass members are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful intrusion into of their private Internet communications.

FIFTH CAUSE OF ACTION

(Statutory Larceny, California Penal Code §§ 484 and 496 Against All Defendants)

154. Plaintiffs, individually and on behalf of the Class and Subclass, incorporate the foregoing allegations as if fully set forth herein.

155. California Penal Code Section 496(a) imposes liability upon

> [e]very person who buys or receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or who conceals, sells, withholds, or aids in concealing, selling, or withholding any property from the owner, knowing the property to be so stolen or obtained . . .

156. California Penal Code Section 484, which defines "theft," states in pertinent part:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent

> representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

157. Pursuant to section 484(a), those who defraud others of personal property "by . . . false . . . representation or pretense . . . [are] guilty of theft." Cal. Penal Code § 484.

158. Under California law, Plaintiffs' and Class and Subclass members' personal information constitutes property that may be the subject of theft.

159. Gen Digital and Avast acted in a manner constituting theft, in violation of § 496(a), by making false or fraudulent representations or pretenses to defraud Plaintiffs and Class and Subclass members of their personally-identifiable information.

160. To induce Plaintiffs and Class and Subclass members to use Gen Digital and Avast products—a necessary component of Gen Digital and Avast's scheme to steal its users' personal information—Gen Digital and Avast use misleading and false product names and advertising claims to (i) intentionally misrepresent that their products make it safer and more secure to browse the Internet and (ii) promise to keep Plaintiffs' and Class and Subclass members' online communications safe and secure from data harvesters. Gen Digital and Avast knowingly make these false representations with the intent that Plaintiffs and Class and Subclass members will rely on them as true and use Gen Digital and Avast's products. Choosing to install and use Gen Digital and Avast's products demonstrates Plaintiffs' and Class and Subclass Members' reliance on Gen Digital and Avast's false representations regarding the safety and security of their data.

161. Despite Gen Digital and Avast's false guarantee to the contrary, Gen Digital and Avast knowingly harvested Plaintiffs' and Class and Subclass members' sensitive and valuable Internet browsing data, and sold their data for a profit, without Plaintiffs' and Class and Subclass members' knowledge or consent, and without compensating them.

162. Gen Digital and Avast further violated section 496(a) by receiving, selling, or aiding in selling, concealing, or withholding Plaintiffs' and Class and Subclass members' personal information, knowing that such property was stolen or wrongfully obtained.

163. Gen Digital and Avast knew at the time they received, sold, or aided in selling, concealing, or withholding Plaintiffs' and Class and Subclass members' personal information, that such property was stolen or wrongfully obtained. For example, Gen Digital and Avast's knowledge of this unlawful conduct was evidenced in January 2020, when Avast CEO, Ondrej Vlcek, conceded that "Avast's sale of user data through its subsidiary Jumpshot . . . rightfully raised a number of questions–including the fundamental question of trust."

164. Gen Digital and Avast received, sold, or aided in selling, concealing, or withholding Plaintiffs' and Class and Subclass members' personal information with the intent to deprive Plaintiffs and Class and Subclass members of such personal information permanently or to deprive them of a major portion of the value or enjoyment of such property. Gen Digital and Avast demonstrated this intent by agreeing to wind down Jumpshot but never committing to delete the personal data they collected and shared without the consent of their users or disgorge the profits they garnered by virtue of such unauthorized conduct.

165. Jumpshot violated California Penal Code § 496(a) by buying or receiving Plaintiffs' and Class and Subclass members' personal information that Gen Digital and Avast had stolen or obtained in a manner constituting theft, knowing the property to be so stolen or obtained.

166. Jumpshot further violated § 496(a) by concealing, selling, or withholding, or aiding in concealing, selling, or withholding Plaintiffs' and Class and Subclass members' personal information that Gen Digital and Avast had stolen or obtained in a manner constituting theft, knowing the property to be so stolen or obtained.

167. Plaintiffs and Class and Subclass members' personal data carries tremendous financial value, as evinced by the tens of millions in annual revenue generated by Gen Digital and Avast licensing their users' data to Jumpshot. Further substantiating the economic value of this personal data, in December 2018, a major marketing provider paid Jumpshot $6.5 million for a three-year supply of the daily click-stream data generated by Gen Digital and Avast users.

168. Plaintiffs and Class and Subclass members did not consent to the extraction and sale of their detailed Internet browsing data, nor did they have any control over its use to produce revenue; therefore, Defendants' profits on such personal data were unjustly earned.

169. Plaintiffs and Class and Subclass members retain a stake in the unjustly earned profits Defendants derived from their violations of California Penal Code § 496(a).

170. While the exact value of Plaintiffs' and Class and Subclass members' personal information in this action will be a matter for expert determination, it is clear that Defendants have been unjustly enriched by the practices described herein and Plaintiffs and Class and Subclass members have a right to disgorgement and/or restitution damages for the value of their stolen data.

171. Pursuant to Penal Code § 496(c), Plaintiffs and Class and Subclass members are entitled to treble damages, as well as attorneys' fees and costs, for injuries sustained as a result of Defendants' violations of § 496(a).

SIXTH CAUSE OF ACTION

**(Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*.
Against All Defendants)**

172. Plaintiffs, individually and on behalf of the Class and Subclass, incorporate the foregoing allegations as if fully set forth herein.

173. The California Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200. Defendants have violated the UCL.

174. Defendants' "unlawful" acts and practices include:

a. Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq*. (Gen Digital and Avast);

b. Violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 631 and 632 (Gen Digital and Avast);

c. Invasion of Privacy under Article I, § 1 of the California Constitution (All Defendants);

d. Intrusion Upon Seclusion (All Defendants);

e. Statutory Larceny, California Penal Code §§ 484 and 496 (All Defendants).

175. All Defendants violated the "unlawful" prong of the UCL through their violation of statutes, Constitutional provisions, and common law, as alleged above.

176. All Defendants violated the "unfair" prong of the UCL because they intercepted communications, or knowingly received intercepted communications, containing the private and personally-identifiable information of Plaintiffs and Class and Subclass members under circumstances in which Plaintiffs and Class and Subclass members would have no reason to know that such information was being intercepted because it was never disclosed or otherwise made known to them by Defendants. To establish liability under the unfair prong, Plaintiffs and Class and Subclass members need not establish that these statutes were actually violated, although the claims pleaded herein do so.

177. All Defendants also violated the "unfair" prong of the UCL because their business acts and practices are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of the harm posed and caused by Defendants secretly collecting or receiving data about Plaintiffs and the Class and Subclass members is significant, and there is no corresponding benefit resulting from such conduct. Because Plaintiffs and the Class and Subclass members were completely unaware of Defendants' conduct, they could not have avoided the harm.

178. Plaintiffs and Class and Subclass members have suffered injury-in-fact, including the loss of money and/or property as a result of Defendants unfair and/or unlawful practices, to wit, the unauthorized collection of their personal information which has value in an amount to be proven at trial. Moreover, Plaintiffs and Class and Subclass members have suffered harm in the form of diminution of the value of their private and personally-identifiable data and content.

179. Defendants' actions caused damage to and loss of Plaintiffs' and Class and Subclass members' property right to control the dissemination and use of their personal information and communications.

180. Defendants have taken property from Plaintiffs and the Class and Subclass members without providing just, or any, compensation.

181. Defendants should be required to cease their unfair and/or illegal collection of user data and to retrieve and delete all unfairly and/or illegally obtained user data.

182. Defendants reaped unjust profits and revenues in violation of the UCL. Plaintiffs and Class and Subclass members seek injunctive relief governing Defendants' ongoing taking and

possession of their information, or failure to account to Plaintiffs, the Class and the Subclass concerning their possession and use of their data, and restitution and disgorgement of these unjust profits and revenues.

183. Plaintiffs, the Class, and the Subclass lack an adequate remedy at law because the ongoing harms from Defendants' taking, possession, and use of data must be addressed by injunctive relief and, due to the ongoing and nature of the harm, cannot be adequately addressed by monetary damages alone.

SEVENTH CAUSE OF ACTION

(Unjust Enrichment
Against All Defendants)

184. Plaintiffs, individually and on behalf of the Class and Subclass, incorporate the foregoing allegations as if fully set forth herein.

185. Plaintiffs and Class and Subclass members conferred a benefit on Defendants in the form of highly personal web browsing data which has substantial monetary value that Defendants extracted and used to produce revenue and unjustly retained those benefits at the expense of Plaintiffs and Class and Subclass members.

186. Defendants collected, licensed, packaged and/or used this information for their own gain, reaping economic, intangible, and other benefits, including substantial monetary compensation from those who purchase or obtain access to Plaintiffs' and Class and Subclass members' personal web browsing data.

187. Defendants unjustly retained those benefits at the expense of Plaintiffs and Class and Subclass members because Defendants' conduct damaged Plaintiffs and Class and Subclass members, all without providing any commensurate compensation to Plaintiffs and Class and Subclass members.

188. Plaintiffs and Class and Subclass members did not consent to the extraction and sale of their detailed Internet browsing data, nor did they have any control over its use to produce revenue. Therefore, under principles of equity and good conscience, Defendants should not be permitted to retain any money derived from their provision, licensing, or sale of information to

Jumpshot or any third party, and Defendant Jumpshot should not be permitted to retain any money derived from its receipt or sale of Plaintiffs' and Class and Subclass members' personal Internet browsing data.

189. The benefits that Defendants derived from Plaintiffs and Class and Subclass members rightly belong to Plaintiffs and Class and Subclass members. It would be inequitable under unjust enrichment principles to permit Defendants' retention of any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request relief against Defendants as set forth below:

a. entry of an order certifying the proposed class and subclass pursuant to Federal Rule of Civil Procedure 23;

b. entry of an order appointing Plaintiffs as representative of the Class and Subclass;

c. entry of an order appointing Plaintiffs' counsel as co-lead counsel for the Class and Subclass;

d. entry of an order for injunctive and declaratory relief as described herein, including but not limited to:

i. enjoining Defendants from continuing to intercept, receive, and/or collect electronic communications of user information, browsing history, search history, and/or web activity;

ii. enjoining Defendants from transmitting any additional user data to any person or entity;

iii. enjoining Defendants from taking and transmitting to anyone else the above-described user data;

iv. requiring Defendants to provide Plaintiffs with credit monitoring services;

v. requiring Defendants to return or destroy any and all data that was sold by Defendants;

vi. requiring Defendants to destroy the user data taken pursuant to the above

practices, including that user data in the possession of third parties;

vii. requiring Defendants to provide confirmation that the above steps have been implemented;

viii. requiring Defendants to provide each consumer whose information was unlawfully collected with notice of who that information was communicated to;

e. entry of judgment in favor of each Class and Subclass member for damages suffered as a result of the conduct alleged herein, punitive damages, restitution, and disgorgement, to include interest and prejudgment interest;

f. leave to amend this Complaint to conform to the evidence produced at trial;

g. award Plaintiffs and Class and Subclass members their reasonable costs and expenses incurred in this action, including attorneys' fees and costs; and

h. grant such other and further legal and equitable relief as the court deems just and equitable.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

DATED: December 19, 2022

Ekwan E. Rhow
Marc E. Masters
Oliver Rocos
BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW, P.C.

By: */s/ Ekwan E. Rhow*

Attorneys for Plaintiffs

DATED: December 19, 2022

Jonathan M. Rotter
David J. Stone
GLANCY PRONGAY & MURRAY LLP

By: */s/ Jonathan M. Rotter*

Attorneys for Plaintiffs

DATED: December 19, 2022

Korey A. Nelson
Amanda K. Klevorn
Claire E. Bosarge
BURNS CHAREST LLP

By: */s/ Korey A. Nelson*

Attorneys for Plaintiffs

Pursuant to Civil L.R. 5-1(h)(3), all signatories concur in filing this stipulation.

Dated: December 19, 2022

s/ Jonathan M. Rotter
Jonathan M. Rotter